6400-11wous dkh 12/21/00

File 351:Derwent WPI 1963-2000/UD,UM &UP=200065
(c) 2000 Derwent Info Ltd
*File 351: Number of updates increased to 67 for 2000.
Please enter HELP NEWS 351 for details.

Set	Items	Description
S1	1	PN=DE 19718547

1/5/1
DIALOG(R)File 351:Derwent WPI
(c) 2000 Derwent Info Ltd. All rts. reserv.

012178945 **Image available**
WPI Acc No: 1998-595856/*199851*
XRPX Acc No: N98-463645
System for secure reading and processing of data on intelligent data media - uses code stored on IC cards in addition to data to be read and identification data and provides code to master centre terminals for authentication of data media using symmetrical encoding technique
Patent Assignee: DEUT TELEKOM AG (DEBP)
Inventor: SCHAEFER-LORINSER F
Number of Countries: 025 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 19718547	A1	19981112	DE 1018547	A	19970502	199851 B
WO 9850894	A1	19981112	WO 98EP2205	A	19980415	199851
EP 990226	A1	20000405	EP 98919270	A	19980415	200021
			WO 98EP2205	A	19980415	

Priority Applications (No Type Date): DE 1018547 A 19970502
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19718547	A1		8	G07F-007/08	
EP 990226	A1	G		G07F-007/08	Based on patent WO 9850894
WO 9850894	A1	G		G07F-007/08	

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated States (National): CA CN JP KR TR US
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

THIS PAGE BLANK (USPTO)

Abstract (Basic): DE 19718547 A

The system has a master centre (1) with terminals (2a,2b) having an interface (E,D) suitable for temporary communications with the IC cards (4). A code stored on the cards in addition to the data to be read and identification data is available to the terminals for authentication of the data media according to a symmetrical encoding technique.

Each card contains an individual code pair which satisfies the conditions for an asymmetrical code algorithm. The first code remains on the card as a signature function. The second code is passed to the reading terminal as a verification function for reading data media by testing the signature electronically transferred to the terminal.

USE - Especially for IC cards.

ADVANTAGE - Increases security against duplicating data media used in system.

Dwg.1/2

Title Terms: SYSTEM; SECURE; READ; PROCESS; DATA; INTELLIGENCE; DATA; MEDIUM; CODE; STORAGE; IC; CARD; ADD; DATA; READ; IDENTIFY; DATA; CODE; MASTER; CENTRE; TERMINAL; AUTHENTICITY; DATA; MEDIUM; SYMMETRICAL; ENCODE
; TECHNIQUE
Derwent Class: T01; T05; W01
International Patent Class (Main): G07F-007/08
International Patent Class (Additional): G07C-009/00; G07F-019/00; H04L-009/32
File Segment: EPI

THIS PAGE BLANK (USPTO)

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Offenlegungsschrift

(10) DE 197 18 547 A 1

(51) Int. Cl.[6]:
G 07 F 7/08
G 07 F 19/00
G 07 C 9/00
H 04 L 9/32

(21) Aktenzeichen: 197 18 547.9
(22) Anmeldetag: 2. 5. 97
(43) Offenlegungstag: 12. 11. 98

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(74) Vertreter:
Gornott, D., Dipl.-Ing., Pat.-Anw., 64291 Darmstadt

(72) Erfinder:
Schaefer-Lorinser, Frank, Dr., 64372 Ober-Ramstadt, DE

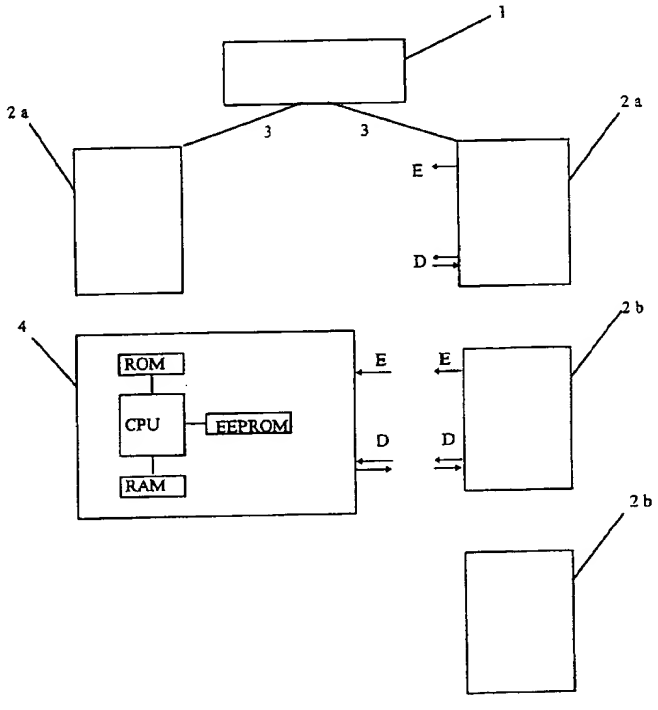
(56) Entgegenhaltungen:
EP 06 54 919 A2
Kryptologie, A. Beutelspacher, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/ Wiesbaden 1994, 4. Aufl., Kap. 5.1, 5.2;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) System zum gesicherten Lesen und Bearbeiten von Daten auf intelligenten Datenträgern

(57) Es werden ein System zum gesicherten Lesen und Bearbeiten von Daten auf intelligenten Datenträgern (4) wie z. B. Chipkarten und in diesem System ausführbare Arbeitsverfahren angegeben, bei denen die gespeicherten Daten und die mit ihnen verbundenen Berechtigungen oder Werte vor dem Zugriff Unbefugter besonders gut geschützt sind. Dies wird durch eine sinnvolle Kombination an sich bekannter Verschlüsselungsverfahren erreicht. Insbesondere wird die Gefahr, die mit dem Ausspähen von in autark arbeitenden Terminals (2b) wie Verkaufsautomaten oder Kartentelefonen hinterlegten, übergeordneten Schlüsseln verbunden ist, beseitigt oder zumindest herabgesetzt und damit einem Mißbrauch der heute zunehmend verwendeten, mit Geldbeträgen aufladbaren Chipkarten entgegengewirkt.



Eingang
14. April 2000

DE 197 18 547 A 1

DE 197 18 547 A 1

Beschreibung

Die Erfindung betrifft ein System zum gesicherten Lesen und Bearbeiten von Daten auf intelligenten Datenträgern gemäß dem Oberbegriff des Patentanspruchs 1 sowie in diesem System ausführbare Verfahren.

Ein System gemäß dem Oberbegriff des Patentanspruch 1 läßt sich z. B. dem Fachbuch "Kryptologie" von A. Beutelspacher, 5. Auflage, Kapitel 4, erschienen 1997 im Vieweg-Verlag, Braunschweig/Wiesbaden, entnehmen und wird als bekannt vorausgesetzt. Insbesondere eignet sich das dort im Zusammenhang mit Bild 4.12 auf S. 93 und Bild 4.16 auf S. 101 beschriebene, auf symmetrischer Verschlüsselung beruhende challenge and response-Verfahren zur Authentikation von intelligenten Datenträgern gegenüber Rechnern oder ihren Eingabeterminals.

Es wurden auch schon Systeme bekannt, die asymmetrische Schlüsselverfahren oder mehrere symmetrische oder asymmetrische Schlüsselverfahren nacheinander einsetzen (siehe z. B. "Funkschau" 1996, Heft 25, S. 60–63). Asymmetrische Schlüsselverfahren, z. B. der in dem eingangs genannten Fachbuch auf S. 122f beschriebene RSA-Algorithmus, haben gegenüber symmetrischen Verfahren aber den Nachteil, daß sie aufgrund von mit sehr großen Zahlen auszuführenden Rechenoperationen relativ langsam sind und, bei Verwendung zur Authentikation der einzelnen Datenträger, die Speicherung vieler Schlüssel in jedem Terminal oder – bei bestehender Datenverbindung zu einem zentralen Speicher – in diesem Speicher voraussetzen.

Die in solchen Systemen verwendeten intelligenten Datenträger, z. B. mit Prozessoren und Speichern ausgestattete IC-Karten – heute meist als Chipkarten bezeichnet –, die oft höchst sensitive Daten wie z. B. Zugangsberechtigungen zu gesicherten Bereichen oder die Erlaubnis zur Abbuchung von Geldbeträgen von einem Konto enthalten, sind infolge der Benutzung der o.g. kryptographischen Verfahren gegen unerlaubte Benutzung, unbefügtes Auslesen wie auch gegen absichtliche Verfälschung der gespeicherten Daten weitgehend gesichert. Dies gilt auch für die heute zunehmend verwendeten, wiederaufladbaren sogenannten elektronischen Geldbörsen (z. B. Pay Card, Geldkarte), von denen zur Bezahlung von Waren oder Dienstleistungen Geldbeträge abgebucht werden können, zumindest dann, wenn die Terminals, an denen die Abbuchungen vorgenommen werden, eine Verbindung zu einer Zentrale aufweisen, über die ein dort gespeicherter, zur Authentikation eines Datenträgers benötigter Schlüssel abgerufen werden kann oder ein von einem Datenträger zur Authentikation übermitteltes Kryptogramm zur Überprüfung an die Zentrale weitergeleitet werden kann.

Letzteres ist jedoch nicht immer der Fall, da Datenverbindungen für öffentliche Kartentelefone, für Fahrkarten-, Parkschein- oder Warenautomaten zu aufwendig sind. Hier wird ein für sicherheitskritische Operationen benötigter Schlüssel meist im Terminal, innerhalb eines sogenannten Sicherheitsmoduls vorgehalten. Dieser Schlüssel ist in aller Regel ein übergeordneter Schlüssel (Master-Key), aus dem der für den jeweils zu bearbeitenden Datenträger benötigte, zu dessen individuellem Schlüssel passende Schlüssel unter Verwendung einer vom Datenträger übermittelten datenträgerindividuellen Information, z. B. der Chipkartennummer, berechnet wird.

Die Tatsache, daß sich dieser übergeordnete Schlüssel in einem Terminal in ungesicherter Umgebung befindet, beeinträchtigt die Sicherheit des gesamten Systems, da sein Ausspähen einen Angreifer in die Lage versetzen würde, zu allen im System verwendeten Datenträgern unberechtigte Duplikate herstellen zu können.

Eine solche Gefahr auszuschließen oder zumindest zu verringern und damit die Sicherheit des Systems zu erhöhen, ist die Aufgabe der vorliegenden Erfindung.

Ein System, das diese Aufgabe löst, wird durch die Merkmale des Patentanspruchs 1 beschrieben.

Arbeitsverfahren für dieses System sind, für den Fall des Auslesens von Daten in den Patentansprüchen 8 und 10, für den Fall der Bearbeitung der auf dem Datenträger enthaltenen Daten in den Patentansprüchen 9 und 11 angegeben, wobei die Patentansprüche 10 und 11 das im Patentanspruch 2 enthaltene, eine Zertifizierung der Datenträger bewirkende Merkmal voraussetzen.

Durch Speicherung eines zweiten, einem asymmetrischen Schlüsselalgorithmus genügenden Schlüsselpaares auf dem Datenträger wird die Möglichkeit geschaffen, am Ende eines Datenauslese- oder -bearbeitungsvorgangs den Vorgang mittels einer sogenannten elektronischen Unterschrift zu bestätigen. Deren Berechnung und Prüfung setzt das auf dem Datenträger gespeicherte Schlüsselpaar voraus und ist nicht allein mittels eines aus dem übergeordneten Schlüssel eines Terminals abgeleiteten Schlüssels und dessen Nachbildung auf dem Datenträger zu erreichen.

Vorteilhafte Weiterbildungen des Systems nach der Erfindung sind in den Unteransprüchen angegeben:

So ermöglicht die in Patentanspruch 2 angegebene Weiterbildung der Erfindung die Überprüfung der Zugehörigkeit der einzelnen Datenträger zum System mittels eines asymmetrischen Schlüsselverfahrens, ohne jedoch die Nachteile eines asymmetrischen Schlüsselverfahrens, wie sie etwa die Hinterlegung geheimer Schlüssel für alle Datenträger an zentraler Stelle mit sich bringen würde, in Kauf zu nehmen. Auch die Richtigkeit des auf dem Datenträger gespeicherten, zur Erstellung der elektronischen Unterschrift benutzten Schlüsselpaares wird hier vom System mitzertifiziert. Dabei verbleibt der zur Erstellung des Zertifikats verwendete, geheime Schlüssel in der Zentrale und ist somit gegen fremden Zugriff sicher.

Die Patentansprüche 3 bis 5 enthalten Ausgestaltungen, die zur Authentikation der Datenträger gegenüber einem Terminal die Benutzung eines nach einem symmetrischen Schlüsselalgorithmus arbeitenden Schlüsselverfahrens gestatten. Die Ableitung der zur Authentikation der einzelnen Datenträger verwendeten Schlüssel aus einem übergeordneten Schlüssel erspart die Online-Anbindung aller Terminals an die Zentrale bzw. die Speicherung umfangreicher Schlüssellisten in den Terminals. Die in den Patentansprüchen 4 und 5 beschriebenen Varianten der Speicherung und/oder Berechnung des zur Authentikation verwendeten Schlüssels auf dem Datenträger erlauben eine Anpassung des Authentikationsvorganges an die technischen Möglichkeiten (Rechen- und Speicherkapazität) der verwendeten Datenträger.

Die Patentansprüche 6 und 7 betreffen die Bereitstellung eines weiteren in einem symmetrischen Schlüsselverfahren verwendbaren Schlüssels.

Die den Verfahrensansprüchen zugeordneten Unteransprüche 12 und 13 betreffen Maßnahmen zur besseren Kontrolle von Buchungsvorgängen bei als elektronische Geldbörsen eingesetzten Datenträgern.

Anhand von zwei Figuren sollen nun Ausführungsbeispiele für das System nach der Erfindung und in diesem System durchgeführte Verfahren zum Auslesen und Bearbeiten der auf Datenträgern gespeicherten Daten beschrieben werden.

Es zeigen:

Fig. 1 schematisch die wesentliche Hardware eines Systems nach der Erfindung,

Fig. 2 ein Ablaufdiagramm für die gesicherte Änderung der auf einem Datenträger eines nach Patentanspruch 7 aus-

gestalteten Systems befindlichen Daten.

In **Fig. 1** ist eine Zentrale **1** dargestellt, welche mit Eingabeeinrichtungen (Terminals) **2a** einer ersten Art über Datenleitungen verbunden ist. Terminals **2b** einer zweiten Art haben keine ständige Verbindung zur Zentrale, sind aber in der Lage, wie die Terminals der ersten Art mit zum System gehörigen Datenträgern **4** zu kommunizieren. Die Datenträger werden hierzu vom jeweiligen Benutzer in eine geeignete Aufnahme eines Terminals gesteckt und dadurch über eine Energieübertragungs-Schnittstelle E mit der Stromversorgung des Terminals und über eine Datenschnittstelle D mit einem im Terminal befindlichen Rechnersystem verbunden. Hierbei kann die Energie- und Datenübertragung in bekannter Weise über elektrische Kontakte, induktiv oder optisch erfolgen. Der Datenträger **4** selbst, in der Regel eine IC-Karte oder Chipkarte, ist mit einem kompletten, einen Prozessor CPU und verschiedene Speicher ROM, RAM, EEPROM enthaltenden Mikrorechnersystem ausgestattet.

Die Datenträger können unterschiedliche, durchaus auch mehrere verschiedene Aufgaben wahrnehmen. Dies kann z. B. eine Ausweisfunktion sein, wo auf dem Datenträger gespeicherte Daten dem Benutzer Zutritt zu einem gesicherten Bereich gewähren oder die Erlaubnis zu einer bestimmten Handlung geben. Bei einer Scheckkarte enthalten die gespeicherten Daten, ggf. in Kombination mit einer vom Benutzer einzugebenden Geheimzahl, die Berechtigung, von einem Konto abzubuchen. – In den genannten Fällen wird man zur Datenauswertung wohl ausschließlich Terminals mit ständiger Datenverbindung zur Zentrale verwenden, was die Bereithaltung von zur Sicherung der Daten vor Manipulation oder unerlaubtem Auslesen erforderlichen Schlüsseln an zentraler, geschützter Stelle ermöglicht –.

Datenträger im Chipkartenformat eignen sich jedoch auch für die Funktion als elektronische Geldbörse, die, mit einem Geldbetrag aufgeladen, zur Bezahlung von Waren oder Dienstleistungen benutzt werden kann. Während das Laden oder Wiederaufladen hier an besonderen, mit der Zentrale, z. B. einer Bank verbundenen Terminals vorgenommen wird, kann das Abbuchen von Beträgen auch an Warenautomaten, Kartentelefonen, Fahrkarten- oder Parkscheinautomaten erfolgen, die als systemzugehörige Terminals ausgestaltet, jedoch nicht mit der Zentrale verbunden sind.

An solchen Terminals ist die Übertragung eines Schlüssels oder verschlüsselter Daten von oder zur Zentrale nicht möglich und das Terminal muß ohne Unterstützung durch die Zentrale erkennen, ob ein Datenträger zum System gehört, ob ein auf dem Datenträger gespeicherter Betrag für eine vorzunehmende Abbuchung ausreicht und ob eine getätigte Abbuchung auf dem Datenträger korrekt erfolgt ist.

Fig. 2 gibt ein Beispiel für den Ablauf eines Abbuchungsvorgangs auf einer als elektronische Geldbörse ausgestalteten Chipkarte an einem nicht mit der Zentrale verbundenen Terminal wieder.

Hierbei enthält der oberste Absatz des Diagramms die vor der Aktion auf der Chipkarte und im Terminal jeweils gespeicherten, der Sicherung des Vorganges dienenden Daten. In den darunter folgenden Absätzen sind in chronologischer Folge jeweils in der linken Spalte die auf der Chipkarte ablaufenden Vorgänge, in der mittleren Spalte die zwischen Chipkarte und Terminal stattfindenden Übertragungen und in der rechten Spalte die im Terminal ablaufenden Vorgänge wiedergegeben.

Die Chipkarte wurde vor Ausgabe an einen Benutzer von der Zentrale mit einem Zertifikat, einem nach einem asymmetrischen Schlüsselverfahren, z. B. dem bekannten RSA-Algorithmus erstellten, eine elektronische Unterschrift darstellenden Kryptogramm versehen. Das Kryptogramm wurde mit Hilfe der nur in der Zentrale verfügbaren Signierfunktion S_{glob} eines globalen, dem genannten asymmetrischen Schlüsselalgorithmus genügenden Schlüsselpaares S_{glob}, V_{glob} erstellt und enthält neben einer die Chipkarte individuell kennzeichnenden Identifikationsnummer (ID-Nummer) und einer Angabe über die Gültigkeitsdauer $T_{gült}$ die Verifikationsfunktion V_{card} eines kartenindividuellen Schlüsselpaares, das die Chipkarte zur Erstellung von elektronischen Unterschriften nach einem weiteren asymmetrischen Schlüsselverfahren befähigt. Die zugehörige Signierfunktion S_{card} ist gleichfalls auf der Karte gespeichert und verbleibt auf ihr. In einem Speicher der Chipkarte befinden sich außerdem weitere, der Durchführung symmetrischer Schlüsselverfahren wie z. B. DES (Data Encryption Standard), Triple DES oder IDEA dienende, kartenindividuelle Schlüssel K_{auth}, K_{red}, sowie weitere Informationen, wie z. B. der Name des Benutzers, der gespeicherte Geldbetrag und eine Sequenznummer, die die Zahl der getätigten Abbuchungen wiedergibt.

In allen zum System gehörigen Terminals sind der zur Verifikation der Zertifikate der Systemchipkarten notwendige Schlüssel V_{glob} und zwei übergeordnete Schlüssel KM_{auth} und KM_{red} gespeichert. Aus den übergeordneten Schlüsseln können die Terminals durch Verknüpfung dieser Schlüssel mit den Identifikationsnummern der jeweils zu bearbeitenden Karten die auf den Karten gespeicherten, der Ausführung symmetrischer Schlüsselverfahren dienenden Schlüssel K_{auth} und K_{red} nachbilden.

Wird nun die Chipkarte mit einem Terminal in Verbindung gebracht, so erfolgt, sobald die Karte dies – z. B. am Anliegen einer Versorgungsspannung – erkennt, eine Übertragung des Zertifikats an das Terminal. Besitzt dieses den globalen Schlüssel V_{glob}, so kann sein Rechner das Zertifikat verifizieren und erfährt dabei die Identifikationsnummer der Karte, deren Gültigkeit und die Verifikationsfunktion V_{card}. Die Identifikationsnummer und V_{card} werden vom Terminal temporär gespeichert und stehen damit für nachfolgende Kontroll- und Rechenvorgänge zur Verfügung.

Im nächsten Schritt löst das Terminal ein sogenanntes challenge and response-Verfahren aus, indem es in bekannter Weise eine Zufallszahl R_1 generiert und an die Karte übermittelt. Der auf der Chipkarte befindliche Rechner erstellt daraufhin ein Kryptogramm e_1, in dem weitere an das Terminal zu übertragende Daten zusammen mit der Zufallszahl R_1, mit Hilfe des nach einem symmetrischen Schlüsselalgorithmus arbeitenden Schlüssels K_{auth} verschlüsselt sind. Insbesondere enthält dieses Kryptogramm den auf der Chipkarte gespeicherten Geldbetrag, damit das Terminal erfährt, bis zu welcher Höhe Geld von der Karte abgebucht werden kann. Das Kryptogramm e_1 wird nun zusammen mit einer auf der Karte generierten zweiten Zufallszahl R_2, die ein challenge and response – Verfahren in Gegenrichtung einleitet, übertragen.

Während auf der Chipkarte das Kryptogramm e_1 erstellt wurde hat das Terminal aus den beiden übergeordneten Schlüsseln KM_{auth} und KM_{red} mit Hilfe der Identifikationsnummer der Karte die kartenindividuellen Schlüssel K_{auth} und K_{red} berechnet und ist nun in der Lage, das Kryptogramm e_1 zu entschlüsseln. Nachdem es den von der Eingabe des Benutzers am Terminal abhängigen abzubuchenden Betrag kennt, vergleicht es diesen mit dem auf der Karte gespeicherten Betrag und erstellt, sofern dieser nicht niedriger ist, ein Abbuchungskryptogramm e_2, welches neben dem abzubuchenden Betrag die zweite Zufallszahl R_2 enthält. Dieses Kryptogramm wird mit Hilfe des weiteren, nach einem symmetrischen Schlüsselalgorithmus arbeitenden Schlüssels K_{red} berechnet und zusammen mit einer dritten Zufallszahl R_3 an die Chipkarte übertragen. Es ist hier prinzipiell möglich, ohne großen Verlust an Sicherheit, anstelle

des weiteren Schlüssels K_{red} nochmals den Schlüssel K_{auth} zu verwenden und den Schlüssel K_{red} einzusparen.

Im nächsten Schritt erfolgt – nach Entschlüsseln des Kryptogramms e_2 – die eigentliche Abbuchung auf der Chipkarte. Die Chipkarte erstellt hierzu einen Buchungsdatensatz D_B mit dem ursprünglich gespeicherten, dem abgebuchten und dem aktuellen Geldbetrag und im System vorgesehenen weiteren Angaben wie z. B. Buchungs-/Sequenznummer, Buchungsdatum, Währung. Die Chipkarte bestätigt diesen Datensatz mit einer elektronischen Unterschrift, indem sie mit Hilfe der Signierfunktion S_{card} des eingangs genannten, weiteren, nach einem asymmetrischen Schlüsselverfahren arbeitenden Schlüsselpaares ein Quittungskryptogramm e_3 erstellt, in welchem neben dem Buchungsdatensatz und der Identifikationsnummer auch die Zufallszahl R_3 verschlüsselt ist. Nachdem das Terminal die zu S_{card} gehörige Verifikationsfunktion V_{card} temporär gespeichert hat, kann es das Kryptogramm e_3 entschlüsseln und somit den Datensatz und die Authentizität der Daten prüfen. Wird kein Fehler gefunden, so werden die temporär gespeicherte Identifikationsnummer und die Verifikationsfunktion V_{card} gelöscht und die Ausgabe der Ware oder Fahrkarte oder die Schaltung einer vom Benutzer gewählten Telefonverbindung veranlaßt.

In ähnlicher Weise kann das Auslesen einer Information aus einem tragbaren Datenträger, z. B. einer als Ausweis dienenden Chipkarte gesichert werden: Hier authentifiziert sich die Chipkarte zunächst gegenüber der Kontrolleinrichtung (Terminal). Dies geschieht mit Hilfe eines symmetrischen Schlüsselverfahrens. Nachfolgend sendet das Terminal einen nach einem symmetrischen Algorithmus kryptogrammgesicherten Auslesebefehl und mit diesem seine Authentikation an die Chipkarte. Diese übergibt die Information mit einer nach einem asymmetrischen Schlüsselverfahren erstellten digitalen Unterschrift.

Bei besonders hohem Sicherheitsbedürfnis und von der Zentrale abgesetzten, nicht mit dieser verbundenen Terminals kann auch hier ein asymmetrisches, die Übertragung eines Zertifikats ermöglichendes Schlüsselverfahren vorgeschaltet werden. In der Regel wird hier jedoch ein symmetrisches Schlüsselverfahren genügen, da hier die Gefahr der Herstellung von Duplikaten von Chipkarten durch einen Berechtigten kaum gegeben ist und ein Dritter, der sich Zugang zu einem im Terminal gespeicherten Schlüssel verschaffen würde, auch noch in den Besitz einer gültigen Chipkarte gelangen müßte, um die elektronische Unterschrift, die letztlich die mit dem Ausweis verbundene Berechtigung gibt, leisten zu können.

Patentansprüche

1. System zum gesicherten Lesen und Ändern von Daten auf intelligenten Datenträgern (4), insbesondere IC-Karten, mit einer übergeordneten Zentrale (1) zugeordneten, mit zur temporären Kommunikation mit den Datenträgern geeigneten Schnittstellen (E, D) ausgestatteten Terminals (2a, 2b), wobei auf jedem Datenträger neben der auszulesenden oder zu ändernden Information und einer Identifikationsinformation ein Schlüssel (K_{auth}) gespeichert ist, der auch den Terminals zur Authentikation des jeweiligen Datenträgers nach einem symmetrischen Schlüsselverfahren zur Verfügung steht, **dadurch gekennzeichnet**, daß auf jedem Datenträger (4) ein diesem individuell zugeordnetes zusätzliches Schlüsselpaar (S_{card}, V_{card}) gespeichert ist, das den Bedingungen eines asymmetrischen Schlüsselalgorithmus genügt, und von dessen Schlüsseln der erste (S_{card}) als Signierfunktion auf dem Datenträger verbleibt und der zweite (V_{card}) als Verifikationsfunktion vom Datenträger an ein zum Auslesen oder Bearbeiten der auf dem Datenträger gespeicherten Daten berechtigtes Terminal ausgebbar ist und dort zur Überprüfung einer mit Hilfe der Signierfunktion vom Datenträger erstellten und an das Terminal übertragenen elektronischen Unterschrift dient.

2. System nach Patentanspruch 1, dadurch gekennzeichnet, daß ein weiteres, den Bedingungen eines asymmetrischen Schlüsselalgorithmus genügendes Schlüsselpaar (S_{glob}, V_{glob}) vorgesehen ist, dessen erster Schlüssel (S_{glob}) an zentraler Stelle, vorzugsweise in der übergeordneten Zentrale verwahrt wird und zur Zertifizierung der im System verwendbaren Datenträger dient, und dessen zweiter Schlüssel (V_{glob}) in allen zum System gehörigen Terminals hinterlegt ist und der Überprüfung der Zertifikate der Datenträger dient.

3. System nach Patentanspruch 1 oder 2, dadurch gekennzeichnet, daß der in dem symmetrischen Schlüsselverfahren zur Authentikation eines Datenträgers zu benutzende Schlüssel unter Verwendung einer datenträgerindividuellen Information, insbesondere einer Identifikationsnummer aus einem übergeordneten Schlüssel (KM_{auth}) abgeleitet ist, daß dieser übergeordnete Schlüssel in allen zum System gehörenden Terminals gespeichert ist, und der zur Authentikation eines Datenträgers gegenüber einem Terminal benötigte Schlüssel (K_{auth}) jeweils aus dem gespeicherten, übergeordneten Schlüssel und der vom Datenträger übermittelten datenträgerindividuellen Information berechnet wird.

4. System nach Patentanspruch 3, dadurch gekennzeichnet, daß der in dem symmetrischen Schlüsselverfahren zur Authentikation eines Datenträgers zu benutzende Schlüssel (K_{auth}) auf jedem Datenträger in seiner endgültigen Form gespeichert ist.

5. System nach Patentanspruch 3, dadurch gekennzeichnet, daß der in dem symmetrischen Schlüsselverfahren zur Authentikation eines Datenträgers zu benutzende Schlüssel auf jedem Datenträger bei Bedarf aus dem übergeordneten Schlüssel und der datenträgerindividuellen Information berechnet wird.

6. System nach einem der vorstehenden Patentansprüche, dadurch gekennzeichnet, daß auf jedem Datenträger und in jedem Terminal ein weiterer, in einem symmetrischen Schlüsselverfahren verwendbarer Schlüssel (K_{red}) zur Verfügung steht, der der Authentikation des Terminals gegenüber einem mit diesem kommunizierenden Datenträger dient.

7. System nach Patentanspruch 6, dadurch gekennzeichnet, daß der weitere Schlüssel (K_{red}) auf dem Datenträger und im Terminal jeweils gespeichert ist oder aus einem gespeicherten übergeordneten Schlüssel (KM_{red}) unter Verwendung einer datenträgerindividuellen Information abgeleitet wird.

8. Verfahren zum gesicherten Lesen von Daten auf intelligenten Datenträgern in einem System nach einem der vorstehenden Patentansprüche, gekennzeichnet durch folgende Schritte:

- Authentikation des Datenträgers (4) gegenüber dem benutzten Terminal (2b) mit einem symmetrischen Schlüsselverfahren, insbesondere einem sogenannten challenge and response-Verfahren, mit Übergabe vorgegebener, auf dem Datenträger gespeicherter datenträgerindividueller Daten sowie des zweiten, der Verifikation dienenden Schlüssels (V_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares (S_{card},

V_{card}) an das Terminal.

– Übergabe eines mit einem symmetrischen Schlüsselverfahren gesicherten Auslesebefehls des Terminals an den Datenträger wobei das symmetrische Schlüsselverfahren gleichzeitig eine Authentikation des Terminals gegenüber dem Datenträger realisiert.

– Übergabe der auszulesenden Daten zusammen mit einer mit Hilfe des ersten Schlüssels (S_{card}) des zusätzlichen Schlüsselpaares (S_{card}, V_{card}) als Signierfunktion erstellten elektronischen Unterschrift

– Überprüfung der elektronischen Unterschrift mittels des zweiten Schlüssels (V_{card}) des zusätzlichen Schlüsselpaares.

9. Verfahren zum gesicherten Bearbeiten von Daten auf intelligenten Datenträgern, insbesondere Abbuchen von Geldbeträgen von als elektronische Geldbörsen verwendeten Chipkarten, in einem System nach einem der vorstehenden Patentansprüche, gekennzeichnet durch folgende Schritte:

– Authentikation des Datenträgers gegenüber dem benutzten Terminal mit einem symmetrischen Schlüsselverfahren, insbesondere einem sogenannten challenge and response-Verfahren, und Übergabe vorgegebener, auf dem Datenträger gespeicherter datenträgerindividueller Daten sowie des zweiten, der Verifikation dienenden Schlüssels (V_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares (S_{card}, V_{card}) an das Terminal.

– Übergabe eines mit einem symmetrischen Schlüsselverfahren gesicherten Datenänderungsbefehls des Terminals an den Datenträger, wobei das symmetrische Schlüsselverfahren gleichzeitig eine Authentikation des Terminals gegenüber dem Datenträger realisiert.

– Ausführung der Datenänderung in Abhängigkeit von der korrekten Authentikation des Terminals.

– Erstellung und Übergabe eines die Datenänderung dokumentierenden Datensatzes (D_B) mit einer nach einem asymmetrischen Schlüsselverfahren mit Hilfe des ersten Schlüssels (S_{card}) des zusätzlichen Schlüsselpaares berechneten elektronischen Unterschrift.

– Überprüfung der elektronischen Unterschrift und des Datensatzes durch das Terminal mittels des zweiten Schlüssels (V_{card}) des zusätzlichen Schlüsselpaares.

10) Verfahren zum gesicherten Lesen von Daten auf intelligenten Datenträgern in einem System nach einem der Patentansprüche 2 bis 7, gekennzeichnet durch folgende Schritte:

– Übertragung vorgegebener, zusammen mit dem der Verifikation dienenden zweiten Schlüssel (V_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares (S_{card}, V_{card}) auf dem Datenträger gespeicherter und mittels des ersten, an zentraler Stelle verwahrten Schlüssels (S_{glob}) des weiteren, einem asymmetrischen Schlüsselalgorithmus genügenden Schlüsselpaares (S_{glob}, V_{glob}) durch elektronische Unterschrift der Zentrale gesicherter datenträgerindividueller Daten an das Terminal und Verifikation der elektronischen Unterschrift mit Hilfe des in allen Terminals hinterlegten zweiten Schlüssels (V_{glob}) dieses Schlüsselpaares.

– Übergabe eines mit einem symmetrischen Schlüsselverfahren gesicherten Auslesebefehls des Terminals an den Datenträger, wobei das symmetrische Schlüsselverfahren, insbesondere ein sogenanntes challenge and response-Verfahren, gleichzeitig eine Authentikation des Terminals gegenüber dem Datenträger realisiert.

– Übergabe der auszulesenden Daten mit einer auf dem Datenträger mittels des ersten Schlüssels (S_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares nach einem asymmetrischen Schlüsselverfahren erstellten elektronischen Unterschrift.

– Überprüfung der auf dem Datenträger erstellten elektronischen Unterschrift durch das Terminal mittels des zweiten Schlüssels (V_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares.

11. Verfahren zum gesicherten Bearbeiten von Daten auf intelligenten Datenträgern, insbesondere Abbuchen von Geldbeträgen von als elektronische Geldbörsen verwendeten Chipkarten, in einem System nach einem der Patentansprüche 2 bis 7, gekennzeichnet durch folgende Schritte:

– Übertragung vorgegebener, zusammen mit dem der Verifikation dienenden zweiten Schlüssel (V_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares (S_{card}, V_{card}) auf dem Datenträger gespeicherter und mittels des ersten, an zentraler Stelle verwahrten Schlüssels (S_{glob}) des weiteren, einem asymmetrischen Schlüsselalgorithmus genügenden Schlüsselpaares (S_{glob}, V_{glob}) durch elektronische Unterschrift der Zentrale gesicherter datenträgerindividueller Daten an das Terminal und Verifikation der elektronischen Unterschrift mit Hilfe des in allen Terminals hinterlegten zweiten Schlüssels (V_{glob}) dieses Schlüsselpaares.

– Übergabe weiterer auf dem Datenträger gespeicherter Daten in einem eine Sicherung der Daten mittels eines symmetrischen Schlüsselverfahrens vornehmenden Übertragungsverfahren, insbesondere einem vom Terminal veranlaßten sogenannten challenge and response-Verfahren.

– Übergabe eines mit einem symmetrischen Schlüsselverfahren gesicherten Datenänderungsbefehls des Terminals an den Datenträger, wobei das symmetrische Schlüsselverfahren, insbesondere ein challenge and response-Verfahren, gleichzeitig eine Authentikation des Terminals gegenüber dem Datenträger realisiert.

– Ausführung der Datenänderung im Datenträger in Abhängigkeit von der korrekten Authentikation des Terminals.

– Erstellung und Übergabe eines die Datenänderung dokumentierenden Datensatzes (D_B) zusammen mit einer auf dem Datenträger mit Hilfe des ersten Schlüssels (S_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares nach einem asymmetrischen Schlüsselverfahren erstellten elektronischen Unterschrift.

– Überprüfung der auf dem Datenträger erstellten elektronischen Unterschrift und des Datensatzes durch das Terminal unter Verwendung des zweiten Schlüssels (V_{card}) des dem Datenträger individuell zugeordneten zusätzlichen Schlüsselpaares.

12. Verfahren nach Patentanspruch 9 oder Patentanspruch 11, dadurch gekennzeichnet, daß der Datenträ-

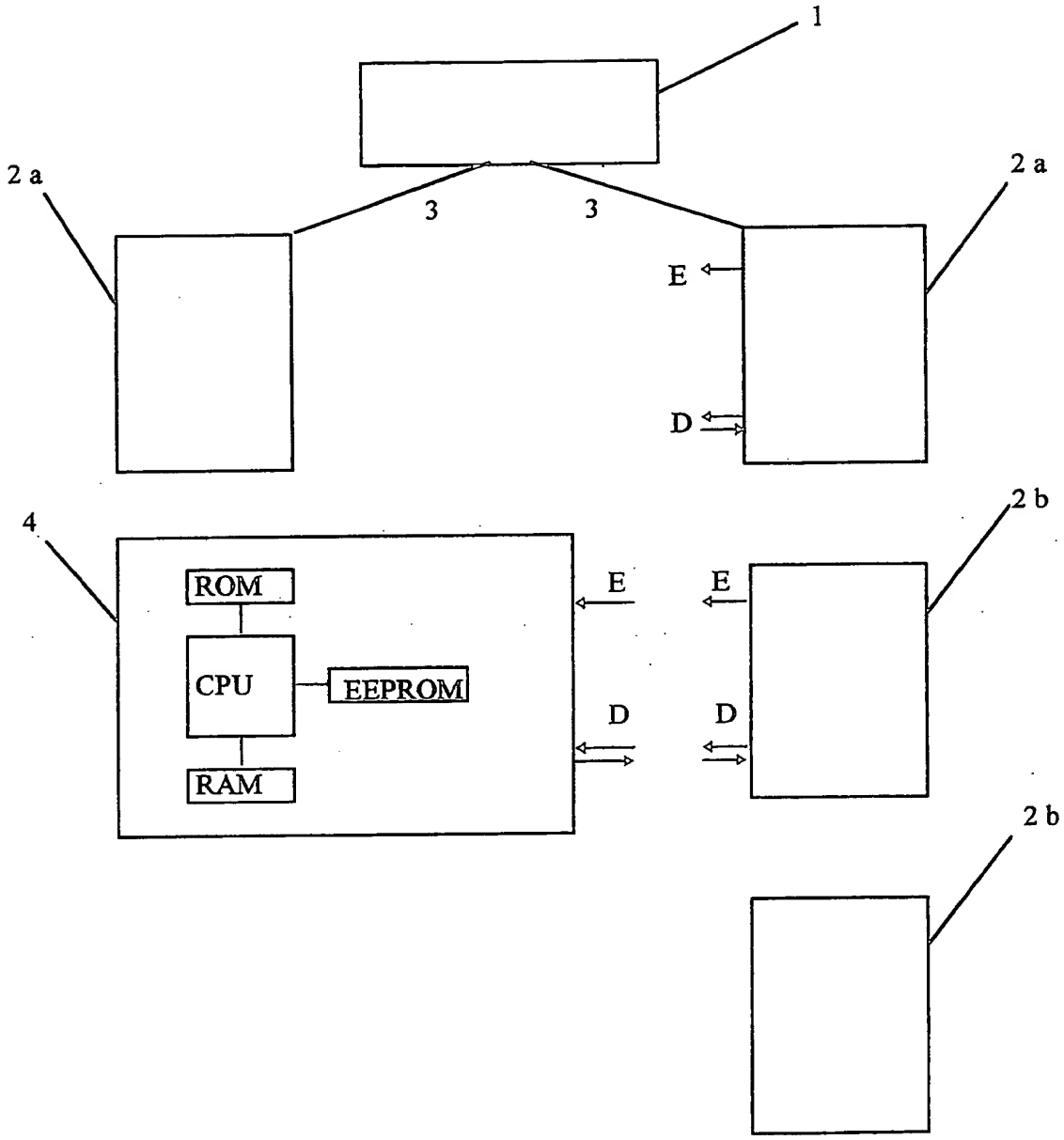
ger als elektronische Geldbörse verwendet wird und daß der die Datenänderung dokumentierende Datensatz (D_B) den vor der Bearbeitung der Daten (Abbuchung) gültigen Geldbetrag, den abgebuchten Geldbetrag und den nach der Bearbeitung der Daten gültigen Geldbetrag enthält.

13. Verfahren nach einem der Patentansprüche 9, 11 oder 12, dadurch gekennzeichnet, daß die Anzahl der Datenbearbeitungen auf dem Datenträger fortlaufend gezählt und eine das Zählergebnis wiedergebende Sequenznummer zusammen mit dem die Datenänderung dokumentierenden Datensatz auf das Terminal übertragen wird.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 197 18 547 A1
Int. Cl.[6]: G 07 F 7/08
Offenlegungstag: 12. November 1998

Figur 1



Num
Int. Cl.:
Offenlegungstag:

DE 197 18 547 A1
G 07 F 7/08
12. November 1998

Figur 2

Chipkarte	Übertragung	Terminal
Zertifikat: S_{glob} (ID-Nr., V_{card}, $T_{gült}$) K_{auth}, K_{red}, S_{card}, Name, Betrag, Sequenznr., ggf. weitere Info		V_{glob}, KM_{auth}, KM_{red}
	Zertifikat ⇒	
		Überprüfen d. Zertifikats mit V_{glob}, temporär. Speichern von V_{card} und ID - Nummer, Generieren einer Zufallszahl R_1
	⇐ R_1	
Erstellen eines Kryptogrammes: $e_1 = K_{auth}$ (ID - Nr., R_1, Betrag, weitere Info), Generieren von R_2		Berechnen von K_{auth} aus KM_{auth} und ID - Nummer und K_{red} aus KM_{red} und ID - Nummer
	e_1, R_2 ⇒	
		Entschlüsseln von e_1 mittels K_{auth} Feststellen ob Abbuchung möglich Erstellen eines Kryptogramms $e_2 = K_{red}$ (Abb.-Betrag, R_2) Generieren von R_3
	⇐ e_2, R_3	
Entschlüsseln von e_2 mittels K_{red} Abbuchung ausführen, Buchungs - datensatz D_B erstellen, Elektron. Unterschrift mit S_{card} berechnen : $e_3 = S_{card}$ (ID-Nr., D_B, R_3)		
	e_3 ⇒	
		Prüfen der Elektronischen Unter - schrift durch Entschlüsseln mit temporär.gespeichertem V_{card}, Wenn Unterschrift und Buchungs- daten o.k., V_{card} u. ID-Nr. löschen, Ware, Fahrkarte o.ä. ausgeben.